

BAB VI PENUTUP

Bab ini berisi tentang beberapa kesimpulan yang dihasilkan berdasarkan penelitian yang telah dilaksanakan. Di samping itu, pada bab ini juga dimasukkan beberapa saran yang dapat digunakan jika penelitian ini ingin dikembangkan.

6.1 Kesimpulan

Berdasarkan analisis terhadap hasil pengujian sistem kriptanalisis RSA dengan menggunakan jaringan syaraf tiruan back propagation, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Learning rate berpengaruh terhadap lama waktu dan jumlah epoch yang dibutuhkan untuk proses training. Semakin besar learning rate, semakin cepat waktu yang dibutuhkan dan semakin sedikit epoch yang dibutuhkan untuk proses training. Dari penelitian yang dilakukan, didapatkan bahwa learning rate $\alpha=1$ adalah yang paling efisien.
2. Meskipun membutuhkan epoch yang cukup banyak dan waktu yang cukup lama untuk proses training, namun back propagation memiliki tingkat keberhasilan training mencapai 99%.
3. Waktu yang dibutuhkan jaringan syaraf tiruan back propagation untuk mendekripsi cipherteks hampir sama dengan waktu mendekripsi dengan menggunakan algoritma RSA itu sendiri.

6.2 Saran

Dalam penulisan tugas akhir terdapat banyak sekali kekurangan dan ketidaksempurnaan, oleh karena itu saran bagi pengembangan perancangan aplikasi jaringan syaraf tiruan ini perlu dilakukan untuk memaksimalkan hasil dan kelayakan aplikasi. Dengan melihat hasil yang dicapai pada penelitian ini, ada beberapa hal yang penulis sarankan untuk pengembangan selanjutnya yaitu:

1. Menambah jumlah percobaan di dalam data pelatihan dan kriptanalisis dengan kunci yang lebih bervariasi agar didapatkan keakuratan yang lebih baik.
2. Pada pengembangan berikutnya dapat juga digunakan sistem database agar dapat mempelajari jenis-jenis chiperteks dengan kombinasi kunci publik yang lebih banyak lagi dan dapat disimpan.
3. Dilakukan penelitian lebih lanjut dengan menggunakan metode pelatihan Jaringan Syaraf Tiruan yang lain sehingga dapat dibandingkan tingkat keakuratan secara keseluruhan.
4. Menambahkan digit bilangan prima yang digunakan untuk kunci. Karena pada dasarnya RSA diakui keamanannya karena sulitnya mendapatkan bilangan prima yang sangat besar sebagai kuncinya karena memiliki digit berjumlah ratusan.